REMARKS/ARGUMENTS

Claims 1-25 have been withdrawn from consideration. Claims 49-50 have been canceled. The Examiner rejected the claims 26-50 under 35 U.S.C. 103(a) as being unpatentable over Hawe (USPN 5,070,528) in view of Hagerman (USPN 6,973,568).

Hagerman states "A Fibre Channel storage area network utilizes frames having time-of-transmission and authentication-code fields. These fields are in addition to the normal fields of Fibre Channel frame headers, and may be implemented as a higher-level protocol encapsulated in the data portion of each frame or may be embedded in an enhanced frame header. The time-of-transmission field is derived from a real-time clock on each node." (column 3, lines 23-33).

Hawe states "More specifically, the offset field included in the cryptographic preamble indicates a number of data elements to skip to the start of the material to be cryptographically processed. In the method of the invention, this offset is used to skip over header information in the packet, which may vary in length and content depending on the protocol under which the packet was generated. The cryptographic preamble further includes a mode field indicating the type of cryptographic processing to be performed, and the step of performing the cryptographic processing includes conditioning the cryptographic processor to perform the type of processing requested in the mode field." (column 3, lines 36-64) The Examiner relies on Hawe to describe "receiving a frame at a first network entity from the second network entity in a fibre channel network" and "identifying a security control indicator in the frame from the second network entity, wherein the security control indicator is used to determine if the frame is encrypted and authenticated." The Examiner argues that Hawe has a cryptographic preamble and an offset field included in the cryptographic preamble that operates as a "security control indicator."

The Examiner argues that a "security control indicator" recited in the claims is anticipated because Hawe describes a cryptographic preamble. The Applicants respectfully disagree. The cryptographic preamble and offset field are not transmitted in any frame as recited in the independent claims. The independent claims explicitly recite receiving a frame at a first network entity from the second network entity and identifying a security control indicator in the frame from the second network entity. Hawe does not teach or suggest any security control indicator that can be transmitted to a first network entity from a second network entity. Even if the cryptographic preamble and the included offset field are assumed to be the security control

indicator, the cryptographic preamble is not received at a second network entity from a first network entity in a fibre channel fabric.

However, Hawe explicitly requires "stripping the cryptographic preamble from the packet if the packet is to be transmitted onto the network, to preserve compatibility with existing packet formats transmitted over the network." (column 3, lines 22-23) Hawe not only does not teach or suggest all of the elements of the independent claims, Hawe actually teaches away from the techniques and mechanisms of the present invention because Hawe suggests that any security control indicator such as a cryptographic preamble has to be stripped from the packet before transmitting the packet "to preserve compatibility with existing packet formats transmitted over the network." By contrast, the independent claims recite a "security control indicator" that is included in a frame transmitted between two network entities in a fibre channel network. Hawe further emphasizes this aspect by stating "The header does not affect packet formats transmitted on a network, because it (the cryptographic header) is stripped off the packet prior to transmission." (column 19, lines 27-30)

Nonetheless, the claims have been amended to facilitate prosecution. The independent claims all recite a first frame having a security enable indicator and a second frame having a security control indicator. The amendments are believed supported in Figure 4 and associated description. For example, "At 411, the network entity 401 transmits a message such as a PLOGI or FLOGI, or other ad hoc messages with a security enable parameter to a network entity 403. The authentication message can contain an identifier such as a user name or an authentication identifier that allows the receiver to select an authentication mechanism out of a possible set of mechanisms. According to various embodiments, to allow authentication, network entity 403 already has a user name, a salt, and a verifier derived from the salt and the password associated with the user name. If the network entity 403 supports security, the network entity 403 identifies the security enable parameter and transmits an acknowledgement at 415 to network entity 401 indicating support for security. According to various embodiments, the transmission at 415 includes a salt parameter." (page 12, lines 2-12)

In addition "The techniques of the present invention include security in initialization messages such as PLOGI, FLOGI, and other classes of messages such as SW_ILS, FC-CT, ELS and ELP. According to various embodiments, the techniques of the present invention embed a security enable parameter in an authentication message. When a new network entity is

introduced into a fibre channel fabric, the new network entity transmits an initialization message with the security enable parameter. The receiving network entity may or may not support security. If the receiving network entity supports authentication, the receiving network entity can extract the security enable parameter and transmit a response acknowledging authentication capabilities. Other information can be exchanged during an authentication sequence to provide for future security in transmissions between the two network entities. In one example, the two entities can exchange cryptographic material in the authentication sequence to allow common key generation." (page 11, lines 19-31)

Furthermore, "Any indicator showing that the frame is secure is referred to herein as a security control indicator. It should also be noted that this is distinct from the above mentioned security enable indicator, which is used during an initialization sequence to show whether a newly introduced node supports security." (page 20, lines 3-7)

None of the references either alone or in combination teach or suggest "a first frame associated with a fabric login or port login message" and having a "security enable parameter" and a second frame having a "security control indicator." Furthermore, none of the references either alone or in combination teach or suggest an acknowledgment that a network entity supports security, the "acknowledgment including algorithm information."

In light of the above remarks relating to independent claims, the remaining dependent claims are believed allowable for at least the reasons noted above. Applicants believe that all pending claims are allowable. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
Weaver Austin Villeneuve & Sampson LLP

/Audrey Kwan/

G. Audrey Kwan
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100